

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10327142 A**(43) Date of publication of application: **08 . 12 . 98**

(51) Int. Cl.

**H04L 9/14**  
**G06K 17/00**  
**G09C 1/00**  
**H04L 9/32**

(21) Application number: **09110889**(22) Date of filing: **28 . 04 . 97**(30) Priority: **26 . 03 . 97 JP 09 73205**(71) Applicant: **SONY CORP**

(72) Inventor: **KUSAKABE SUSUMU**  
**ISHIBASHI YOSHITO**  
**TAKADA MASAYUKI**

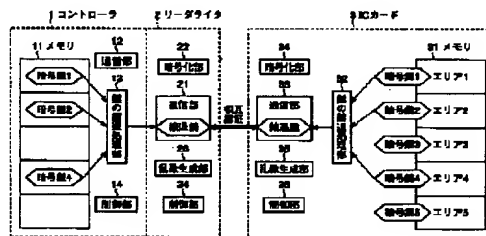
(54) **AUTHENTICATION SYSTEM, ITS METHOD,  
 AUTHENTICATION DEVICE AND ITS METHOD**

(57) Abstract:

**PROBLEM TO BE SOLVED:** To reduce a time required for authentication in the case of conducting authentication by using a plurality of encryption keys.

**SOLUTION:** In the case that encryption keys 1-5 are required respectively to access areas 1-5 of a memory 31 of an IC card 3, a reader/writer 2 reports a plurality of areas to be accessed to the IC card 3, a plurality of encryption keys corresponding to the areas (e.g. encryption keys 1, 2 and 4) are read and a degeneration processing section 32 generates a degeneration key. Furthermore, a random number generated by a random number generating section 23 of the reader/writer 2 is transferred to the IC card 3 and an encryption section 34 encrypts data by using the degeneration key. The reader/writer 2 receives the transferred encrypted random number from the IC card 3, decodes the random number by using the degeneration key and discriminates the IC card 3 to be proper when the decoded random number is equal to the generated random number.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-327142

(43) 公開日 平成10年(1998)12月8日

(51) Int.Cl.<sup>6</sup> 識別記号  
 H 0 4 L 9/14  
 G 0 6 K 17/00  
 G 0 9 C 1/00 6 6 0  
 H 0 4 L 9/32

F I  
 H 0 4 L 9/00 6 4 1  
 G 0 6 K 17/00 T  
 G 0 9 C 1/00 6 6 0 A  
 H 0 4 L 9/00 6 7 5 A

審査請求 未請求 請求項の数25 O L (全 21 頁)

(21) 出願番号 特願平9-110889

(22) 出願日 平成9年(1997)4月28日

(31) 優先権主張番号 特願平9-73205

(32) 優先日 平9(1997)3月26日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 日下部 進

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 石橋 義人

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 高田 昌幸

東京都品川区北品川6丁目7番35号 ソニー株式会社内

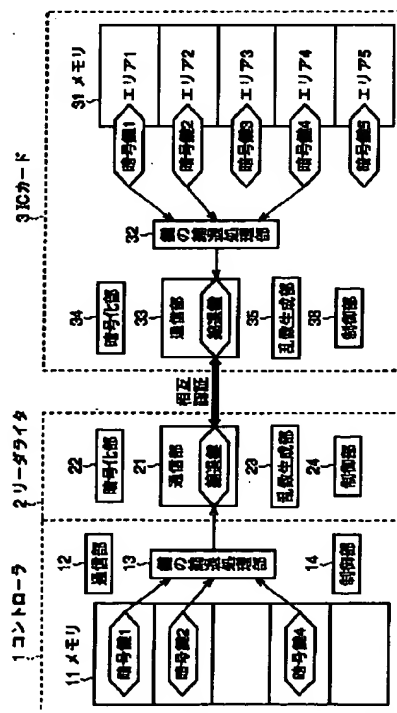
(74) 代理人 弁理士 稲本 義雄

## (54) 【発明の名称】 認証システムおよび方法、並びに認証装置および方法

## (57) 【要約】

【課題】 複数の暗号鍵を用いて認証を行う場合における認証時間を短くする。

【解決手段】 ICカード3のメモリ31のエリア1乃至エリア5のうち、各エリアアクセスするのに、それぞれ暗号鍵1乃至暗号鍵5が必要である場合、アクセスする複数のエリアを、リーダライタ2からICカード3に通知し、そのエリアに対応する複数の暗号鍵（例えば暗号鍵1、暗号鍵2、および暗号鍵4）を読み出し、縮退処理部32で、それらから1つの縮退鍵を生成させる。また、リーダライタ2の乱数生成部23で生成した乱数をICカード3に転送し、暗号化部34で、縮退鍵を用いて暗号化させる。リーダライタ2は、ICカード3から、この暗号化された乱数の転送を受け、縮退鍵を用いて復号化し、復号化した乱数と発生した乱数とが等しければ、ICカード3が適正なものであるとする。



## 【特許請求の範囲】

【請求項1】 第1の装置と第2の装置との間で認証処理を行う認証システムにおいて、

前記第1の装置は、

複数の鍵を記憶する第1の記憶手段と、

前記第1の記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第1の生成手段と、

前記第2の装置との間で通信を行う第1の通信手段と、を備え、

前記第2の装置は、

複数の鍵を記憶する第2の記憶手段と、

前記第2の記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第2の生成手段と、

前記第1の装置との間で通信を行う第2の通信手段とを備え、

前記第1の装置と第2の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化手段を備え、

前記第1の装置と第2の装置の他方は、前記暗号化手段により暗号化されたデータを前記認証鍵を用いて復号化する復号化手段を備えることを特徴とする認証システム。

【請求項2】 前記第1の装置と第2の装置の一方は、他方に対して、そこに記憶されている複数の前記鍵のうちの任意の数の鍵から、対応する1つの認証鍵を生成するのに必要な情報を通知する通知手段をさらに備え、前記第1の装置と第2の装置の他方は、前記通知手段により通知された情報に対応して前記認証鍵を生成することを特徴とする請求項1に記載の認証システム。

【請求項3】 前記第1の装置と第2の装置の少なくとも一方は、乱数を生成する乱数生成手段を備え、前記暗号化手段は、前記乱数生成手段で生成された乱数を暗号化し、前記復号化手段は、暗号化された前記乱数を復号化することを特徴とする請求項1に記載の認証システム。

【請求項4】 前記第2の装置は、複数の前記鍵に対応する複数の情報記録領域を有することを特徴とする請求項1に記載の認証システム。

【請求項5】 第1の装置と第2の装置との間で認証処理を行う認証方法において、

前記第1の装置は、

複数の鍵を記憶する第1の記憶ステップと、

前記第1の記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第1の生成ステップと、

前記第2の装置との間で通信を行う第1の通信ステップと、

を備え、

前記第2の装置は、

複数の鍵を記憶する第2の記憶ステップと、

前記第2の記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第2の生成ステップと、

前記第1の装置との間で通信を行う第2の通信ステップとを備え、

前記第1の装置と第2の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化ステップを備え、

前記第1の装置と第2の装置の他方は、前記暗号化ステップで暗号化されたデータを前記認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする認証方法。

【請求項6】 他の装置との間で認証処理を行う認証装置において、

前記他の装置との間で通信を行う通信手段と、

複数の鍵を記憶する記憶手段と、

前記記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成手段と、

前記他の装置に対して、前記他の装置に記憶されている複数の前記鍵のうちの任意の数の鍵から、対応する1つの認証鍵を生成するのに必要な情報と、前記認証鍵を用いて暗号化するデータを通知する通知手段と、

前記他の装置が前記認証鍵を用いて暗号化したデータを、前記認証鍵を用いて復号化する復号化手段とを備えることを特徴とする認証装置。

【請求項7】 前記通知手段は、前記暗号化するデータとして、乱数を通知することを特徴とする請求項6に記載の認証装置。

【請求項8】 他の装置との間で認証処理を行う認証方法において、

前記他の装置との間で通信を行う通信ステップと、

複数の鍵を記憶する記憶ステップと、

前記記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成ステップと、

前記他の装置に対して、前記他の装置に記憶されている複数の前記鍵のうちの任意の数の鍵から、対応する1つの認証鍵を生成するのに必要な情報を通知する通知ステップと、

前記他の装置が前記認証鍵を用いて暗号化したデータを、前記認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする認証方法。

【請求項9】 他の装置との間で認証処理を行う認証装置において、

前記他の装置との間で通信を行う通信手段と、

複数の鍵を記憶する記憶手段と、

前記他の装置から通知された情報に基づいて、前記記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成手段と、前記他の

装置から通知されたデータを、前記認証鍵を用いて暗号

化する暗号化手段とを備えることを特徴とする認証装置。

【請求項 1 0】 複数の前記鍵に対応する複数の情報記録領域をさらに有することを特徴とする請求項 9 に記載の認証装置。

【請求項 1 1】 他の装置との間で認証処理を行う認証方法において、

前記他の装置との間で通信を行う通信ステップと、

複数の鍵を記憶する記憶ステップと、

前記他の装置から通知された情報に基づいて、前記記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、1 つの認証鍵を生成する生成ステップと、

前記他の装置から通知されたデータを、前記認証鍵を用いて暗号化する暗号化ステップとを備えることを特徴とする認証方法。

【請求項 1 2】 第 1 の装置と第 2 の装置との間で認証処理を行う認証システムにおいて、

前記第 1 の装置は、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記第 2 の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第 1 の記憶手段と、

前記第 1 の記憶手段に記憶されている前記鍵と、前記個別データとから、認証鍵を生成する第 1 の生成手段と、前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知手段と、

前記第 2 の装置との間で通信を行う第 1 の通信手段とを備え、

前記第 2 の装置は、

複数の鍵と前記共通データを記憶する第 2 の記憶手段と、

前記第 2 の記憶手段に記憶されている複数の前記鍵のうち、前記第 1 の装置の通信手段からの通知に対応するものと、前記共通データとから、前記認証鍵を生成する第 2 の生成手段と、

前記第 1 の装置との間で通信を行う第 2 の通信手段とを備え、

前記第 1 の装置と第 2 の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化手段を備え、

前記第 1 の装置と第 2 の装置の他方は、前記暗号化手段により暗号化されたデータを前記認証鍵を用いて復号化する復号化手段を備えることを特徴とする認証システム。

【請求項 1 3】 前記認証鍵は、第 1 の認証鍵と第 2 の認証鍵で構成され、前記第 1 の生成手段は、前記第 1 の記憶手段に記憶されている、自己に割り当てられている前記鍵と、前記個別データとから、前記第 1 の認証鍵を生成し、自己に割り当てられている前記鍵と、前記第 1 の認証鍵を用いて前記第 2 の認証鍵を生成し、

前記第 2 の生成手段は、前記第 2 の記憶手段に記憶され

ている複数の前記鍵のうち、前記第 1 の装置の通知手段からの通知に対応するものと、前記共通データとから、前記第 1 の認証鍵を生成し、前記第 1 の認証鍵と、前記第 2 の記憶手段に記憶されている複数の前記鍵のうち、前記第 1 の装置の通知手段からの通知に対応するものを用いて前記第 2 の認証鍵を生成し、

前記第 1 の装置と第 2 の装置は、いずれも前記暗号化手段と復号化手段を備え、

前記第 1 の装置と第 2 の装置の一方は、乱数を生成する乱数生成手段をさらに備え、

前記第 1 の装置と第 2 の装置の一方の暗号化手段は、前記乱数生成手段で生成された乱数を前記第 1 の認証鍵を用いて暗号化し、

前記第 1 の装置と第 2 の装置の他方の復号化手段は、前記第 1 の装置と第 2 の装置の一方の暗号化手段により暗号化された前記乱数を前記第 1 の認証鍵を用いて復号化し、

前記第 1 の装置と第 2 の装置の他方の暗号化手段は、前記第 1 の装置と第 2 の装置の他方の復号化手段により復号化された前記乱数を、前記第 2 の認証鍵を用いて暗号化し、

前記第 1 の装置と第 2 の装置の一方の復号化手段は、前記第 1 の装置と第 2 の装置の他方の暗号化手段により暗号化された前記乱数を前記第 2 の認証鍵を用いて復号化することを特徴とする請求項 1 2 に記載の認証システム。

【請求項 1 4】 前記第 1 の装置と第 2 の装置の一方は、他方から、他方の装置に固有の装置識別番号の送信を受け、

前記第 1 の装置と第 2 の装置の他方は、前記第 1 の記憶手段または第 2 の記憶手段に、前記装置識別番号をさらに記憶し、

前記第 1 の装置の第 1 の生成手段と、前記第 2 の装置の第 2 の生成手段は、前記認証鍵を生成するのに、前記装置識別番号をさらに用いることを特徴とする請求項 1 2 に記載の認証システム。

【請求項 1 5】 前記第 1 の装置の第 1 の通信手段は、前記第 2 の装置の第 2 の記憶手段に記憶されている複数の前記鍵のうち、所定の第 1 の鍵を新たな第 2 の鍵で更新する場合、前記第 2 の鍵を前記第 1 の鍵で暗号化した第 1 の暗号化データと、前記第 2 の鍵に対して所定の関係にある第 3 の鍵を前記第 1 の鍵で暗号化した第 2 の暗号化データを、更新する前記鍵の鍵識別番号とともに前記第 2 の装置に送信することを特徴とする請求項 1 2 に記載の認証システム。

【請求項 1 6】 前記第 2 の装置は、前記第 1 の装置の第 1 の通信手段から送信を受けた、前記第 1 の暗号化データと第 2 の暗号化データを、前記鍵識別番号に対応する前記第 1 の鍵を用いて復号化する第 2 の復号化手段と、

10

20

30

40

50

復号化された前記第2の鍵と第3の鍵が所定の関係にあるか否かを判定し、判定結果に対応して前記第1の鍵を前記第2の鍵で更新する更新手段とをさらに備えることを特徴とする請求項15に記載の認証システム。

【請求項17】 第1の装置と第2の装置との間で認証処理を行う認証方法において、

前記第1の装置は、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記第2の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第1の記憶ステップと、

前記第1の記憶ステップで記憶されている前記鍵と、前記個別データとから、認証鍵を生成する第1の生成ステップと、

前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知ステップと、

前記第2の装置との間で通信を行う第1の通信ステップとを備え、

前記第2の装置は、

複数の鍵と前記共通データを記憶する第2の記憶ステップと、

前記第2の記憶ステップで記憶されている複数の前記鍵のうち、前記第1の装置の通信ステップからの通知に対応するものと、前記共通データとから、前記認証鍵を生成する第2の生成ステップと、

前記第1の装置との間で通信を行う第2の通信ステップとを備え、

前記第1の装置と第2の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化ステップを備え、

前記第1の装置と第2の装置の他方は、前記暗号化ステップにより暗号化されたデータを前記認証鍵を用いて復号化する復号化ステップを備えることを特徴とする認証方法。

【請求項18】 他の装置との間で認証処理を行う認証装置において、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶手段と、

前記記憶手段に記憶されている前記鍵と、前記個別データとから、認証鍵を生成する生成手段と、

前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知手段と、

前記他の装置との間で通信を行う通信手段と、

前記認証鍵を用いて暗号化を行う暗号化手段とを備えることを特徴とする認証装置。

【請求項19】 前記生成手段は、前記認証鍵を生成するのに、前記他の装置に固有の装置識別番号をさらに用いることを特徴とする請求項18に記載の認証装置。

【請求項20】 前記通信手段は、前記他の装置に記憶されている複数の前記鍵のうち、所定の第1の鍵を新た

な第2の鍵で更新する場合、前記第2の鍵を前記第1の鍵で暗号化した第1の暗号化データと、前記第2の鍵に対して所定の関係にある第3の鍵を前記第1の鍵で暗号化した第2の暗号化データを、更新する前記鍵の鍵識別番号とともに前記他の装置に送信することを特徴とする請求項18に記載の認証装置。

【請求項21】 他の装置との間で認証処理を行う認証方法において、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶ステップと、前記記憶ステップで記憶されている前記鍵と、前記個別データとから、認証鍵を生成する生成ステップと、前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知ステップと、前記他の装置との間で通信を行う通信ステップと、前記認証鍵を用いて暗号化を行う暗号化ステップとを備えることを特徴とする認証方法。

【請求項22】 他の装置との間で認証処理を行う認証装置において、

複数の鍵と共通データを記憶する記憶手段と、前記記憶手段に記憶されている複数の前記鍵のうち、前記他の装置からの通知に対応するものと、前記共通データとから、認証鍵を生成する生成手段と、前記他の装置との間で通信を行う通信手段と、前記他の装置により暗号化されたデータを前記認証鍵を用いて復号化する復号化手段とを備えることを特徴とする認証装置。

【請求項23】 前記生成手段は、前記認証鍵を生成するのに、前記他の装置からの通知情報以外に、自己に固有の装置識別番号を用いることを特徴とする請求項22に記載の認証装置。

【請求項24】 前記他の装置から、前記記憶手段に記憶されている複数の前記鍵のうち、所定の第1の鍵を新たな第2の鍵で更新するために、前記第2の鍵を前記第1の鍵で暗号化した第1の暗号化データと、前記第2の鍵に対して所定の関係にある第3の鍵を、前記第1の鍵で暗号化した第2の暗号化データを、更新する前記鍵の鍵識別番号とともに送信を受けたとき、前記第1の暗号化データと第2の暗号化データを、更新する前記鍵の鍵識別番号に対応する前記第1の鍵を用いて復号化する第2の復号化手段と、

復号化された前記第2の鍵と第3の鍵が所定の関係にあるか否かを判定し、判定結果に対応して前記第1の鍵を前記第2の鍵で更新する更新手段とをさらに備えることを特徴とする請求項22に記載の認証装置。

【請求項25】 他の装置との間で認証処理を行う認証方法において、

複数の鍵と共通データを記憶する記憶ステップと、前記記憶ステップで記憶されている複数の前記鍵のう

ち、前記他の装置からの通知に対応するものと、前記共通データとから、認証鍵を生成する生成ステップと、前記他の装置との間で通信を行う通信ステップと、前記他の装置により暗号化されたデータを前記認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証システムおよび方法、並びに認証装置および方法に関し、特に、より迅速に、認証を行うことができるようにした、認証システムおよび方法、並びに認証装置および方法に関する。

【0002】

【従来の技術】図20は、ICカードにおける、従来の認証システムの構成例を表している。この構成例においては、ICカード102とリーダライタ101の間で、認証処理を行うようになされている。ICカード102は、情報を記憶するためのエリアが、エリア1乃至エリア5の5つのエリアに区分されている。そして、各エリア毎に、それぞれ異なる暗号鍵1乃至暗号鍵5が対応されている。エリアiをアクセスするには、対応する暗号鍵iが必要となる。

【0003】すなわち、リーダライタ101が、ICカード102の、例えばエリア1にデータを記録するか、あるいは、そこに記録されているデータを読み出す場合、最初に、相互認証処理が行われる。リーダライタ101は、ICカード102が記憶している暗号鍵1乃至暗号鍵5と同一の符号鍵1乃至暗号鍵5を予め記憶している。そして、ICカード102のエリア1にアクセスする場合には、このエリア1に対応する暗号鍵1を読み出し、これを用いて認証処理を行う。

【0004】例えば、リーダライタ101は、所定の乱数を発生し、この乱数とアクセスすべきエリアの番号1をICカード102に通知する。ICカード102においては、通知されてきた番号1のエリアに対応する暗号鍵1を読み出し、その暗号鍵1を用いて、通知されてきた乱数を暗号化する。そして、暗号化した乱数を、リーダライタ101に通知する。リーダライタ101は、この暗号化された乱数を暗号鍵を用いて復号化する。ICカード102に通知した乱数と復号化した乱数とが一致していれば、ICカード102が適正なものであるとの判定を行う。

【0005】同様に、ICカード102は、所定の乱数を発生し、リーダライタ101に出力する。リーダライタ101は、暗号鍵1を用いて、この乱数を暗号化し、暗号化した乱数をICカード102に通知する。ICカード102は、この暗号化された乱数を暗号鍵1を用いて復号化する。そして、復号化された乱数とリーダライタ101に通知した乱数とが一致していれば、リーダライタ101が適正なリーダライタであると判定する。

【0006】以上の処理は、各エリア毎に行われる。

【0007】

【発明が解決しようとする課題】このように、従来のシステムにおいては、相互認証処理が、エリア毎に個別に行われるようになされているため、各エリアに、迅速にアクセスすることが困難である課題があった。その結果、例えば、通勤者が、改札口に設けられているゲートを通過する、比較的短い時間の間に、ICカード102の所定のエリアにリーダライタ101がアクセスし、情報を書き込み、または読み出すことが困難となる課題があった。

【0008】本発明はこのような状況に鑑みてなされたものであり、より迅速な認証ができるようにするものである。

【0009】

【課題を解決するための手段】請求項1に記載の認証システムは、第1の装置は、複数の鍵を記憶する第1の記憶手段と、第1の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第1の生成手段と、第2の装置との間で通信を行う第1の通信手段と、を備え、第2の装置は、複数の鍵を記憶する第2の記憶手段と、第2の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第2の生成手段と、第1の装置との間で通信を行う第2の通信手段とを備え、第1の装置と第2の装置の一方は、認証鍵を用いて暗号化を行う暗号化手段を備え、第1の装置と第2の装置の他方は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段とを備えることを特徴とする。

【0010】請求項5に記載の認証方法は、第1の装置は、複数の鍵を記憶する第1の記憶ステップと、第1の記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第1の生成ステップと、第2の装置との間で通信を行う第1の通信ステップと、を備え、第2の装置は、複数の鍵を記憶する第2の記憶ステップと、第2の記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する第2の生成ステップと、第1の装置との間で通信を行う第2の通信ステップとを備え、第1の装置と第2の装置の一方は、認証鍵を用いて暗号化を行う暗号化ステップを備え、第1の装置と第2の装置の他方は、暗号化ステップで暗号化されたデータを認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする。

【0011】請求項6に記載の認証装置は、他の装置との間で通信を行う通信手段と、複数の鍵を記憶する記憶手段と、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成手段と、他の装置に対して、他の装置に記憶されている複数の鍵のうちの任意の数の鍵から、対応する1つの認証鍵を生成するのに必要な情報と、認証鍵を用いて暗号化するデ

ータを通知する通知手段と、他の装置が認証鍵を用いて暗号化したデータを、認証鍵を用いて復号化する復号化手段とを備えることを特徴とする。

【0012】請求項8に記載の認証方法は、他の装置との間で通信を行う通信ステップと、複数の鍵を記憶する記憶ステップと、記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成ステップと、他の装置に対して、他の装置に記憶されている複数の鍵のうちの任意の数の鍵から、対応する1つの認証鍵を生成するのに必要な情報を通知する通知ステップと、他の装置が認証鍵を用いて暗号化したデータを、認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする。

【0013】請求項9に記載の認証装置は、他の装置との間で通信を行う通信手段と、複数の鍵を記憶する記憶手段と、他の装置から通知された情報に基づいて、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成手段と、他の装置から通知されたデータを、認証鍵を用いて暗号化する暗号化手段とを備えることを特徴とする。

【0014】請求項11に記載の認証方法は、他の装置との間で通信を行う通信ステップと、複数の鍵を記憶する記憶ステップと、他の装置から通知された情報に基づいて、記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、1つの認証鍵を生成する生成ステップと、他の装置から通知されたデータを、認証鍵を用いて暗号化する暗号化ステップとを備えることを特徴とする。

【0015】請求項12に記載の認証システムは、第1の装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、第2の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第1の記憶手段と、第1の記憶手段に記憶されている鍵と、個別データとから、認証鍵を生成する第1の生成手段と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段と、第2の装置との間で通信を行う第1の通信手段とを備え、第2の装置は、複数の鍵と共通データを記憶する第2の記憶手段と、第2の記憶手段に記憶されている複数の鍵のうち、第1の装置の通信手段からの通知に対応するものと、共通データとから、認証鍵を生成する第2の生成手段と、第1の装置との間で通信を行う第2の通信手段とを備え、第1の装置と第2の装置の一方は、認証鍵を用いて暗号化を行う暗号化手段を備え、第1の装置と第2の装置の他方は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段を備えることを特徴とする。

【0016】請求項17に記載の認証方法は、第1の装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、第2の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第1の記憶ス

テップと、第1の記憶ステップで記憶されている鍵と、個別データとから、認証鍵を生成する第1の生成ステップと、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知ステップと、第2の装置との間で通信を行う第1の通信ステップとを備え、第2の装置は、複数の鍵と共通データを記憶する第2の記憶ステップと、第2の記憶ステップで記憶されている複数の鍵のうち、第1の装置の通信ステップからの通知に対応するものと、共通データとから、認証鍵を生成する第2の生成ステップと、第1の装置との間で通信を行う第2の通信ステップとを備え、第1の装置と第2の装置の一方は、認証鍵を用いて暗号化を行う暗号化ステップを備え、第1の装置と第2の装置の他方は、暗号化ステップにより暗号化されたデータを認証鍵を用いて復号化する復号化ステップを備えることを特徴とする。

【0017】請求項18に記載の認証装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶手段と、記憶手段に記憶されている鍵と、個別データとから、認証鍵を生成する生成手段と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段と、他の装置との間で通信を行う通信手段と、認証鍵を用いて暗号化を行う暗号化手段とを備えることを特徴とする。

【0018】請求項21に記載の認証方法は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶ステップと、記憶ステップで記憶されている鍵と、個別データとから、認証鍵を生成する生成ステップと、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知ステップと、他の装置との間で通信を行う通信ステップと、認証鍵を用いて暗号化を行う暗号化ステップとを備えることを特徴とする。

【0019】請求項22に記載の認証装置は、複数の鍵と共通データを記憶する記憶手段と、記憶手段に記憶されている複数の鍵のうち、他の装置からの通知に対応するものと、共通データとから、認証鍵を生成する生成手段と、他の装置との間で通信を行う通信手段と、他の装置により暗号化されたデータを認証鍵を用いて復号化する復号化手段とを備えることを特徴とする。

【0020】請求項25に記載の認証方法は、複数の鍵と共通データを記憶する記憶ステップと、記憶ステップで記憶されている複数の鍵のうち、他の装置からの通知に対応するものと、共通データとから、認証鍵を生成する生成ステップと、他の装置との間で通信を行う通信ステップと、他の装置により暗号化されたデータを認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする。

【0021】請求項1に記載の認証システムおよび請求



項 5 に記載の認証方法においては、複数の鍵から 1 つの認証鍵が生成される。そして、この 1 つの認証鍵を用いて、データが暗号化され、また、復号化される。

【0022】請求項 6 に記載の認証装置および請求項 8 に記載の認証方法においては、複数の鍵を用いて、1 つの認証鍵を生成するのに必要な情報が、他の装置に通知される。そして、他の装置で生成された認証鍵を用いて暗号化されたデータが、認証鍵を用いて復号化される。

【0023】請求項 9 に記載の認証装置および請求項 11 に記載の認証方法においては、他の装置から通知された情報に基づいて、複数の鍵から 1 つの認証鍵が生成される。そして、生成した認証鍵を用いて、データが暗号化される。

【0024】請求項 12 に記載の認証システムおよび請求項 17 に記載の認証方法においては、第 1 の装置に、自己に割り当てられた鍵と、個別データが記憶されており、これらに対応して認証鍵が生成される。第 2 の装置では、第 1 の装置からの通知と、共通データとから、認証鍵が生成される。

【0025】請求項 18 に記載の認証装置および請求項 21 に記載の認証方法においては、共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データが、自己に割り当てられた鍵とともに記憶されている。自己に割り当てられた鍵と、個別データとから、認証鍵が生成される。

【0026】請求項 22 に記載の認証装置および請求項 25 に記載の認証方法においては、他の装置からの通知に対応する鍵と、共通データとから、認証鍵が生成される。

#### 【0027】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定的であることを意味するものではない。

【0028】請求項 1 に記載の認証システムは、第 1 の装置は、複数の鍵を記憶する第 1 の記憶手段（例えば、図 1 のメモリ 11）と、第 1 の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1 つの認証鍵を生成する第 1 の生成手段（例えば、図 1 の縮退処理部 13）と、第 2 の装置との間で通信を行う第 1 の通信手段（例えば、図 1 の通信部 12）と、を備え、第 2 の装置は、複数の鍵を記憶する第 2 の記憶手段（例えば、図 1 のメモリ 31）と、第 2 の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1 つの認証鍵を生成する第 2 の生成手段（例えば、図 1 の縮退処理部 32）と、第 1 の装置との間で通信を行う第 2 の通信手段（例えば、図 1 の通信部 33）とを備え、第 1 の装置と第 2

の装置の一方（例えば、図 1 の IC カード 3）は、認証鍵を用いて暗号化を行う暗号化手段（例えば、図 1 の暗号化部 34）を備え、第 1 の装置と第 2 の装置の他方（例えば、図 1 のコントローラ 1 およびリーダライタ 2）は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段（例えば、図 1 の暗号化部 22）とを備えることを特徴とする。

【0029】請求項 2 に記載の認証システムは、第 1 の装置と第 2 の装置の一方は、他方に対して、そこに記憶されている複数の鍵のうちの任意の数の鍵から、対応する 1 つの認証鍵を生成するのに必要な情報を通知する通知手段（例えば、図 7 のステップ S6）をさらに備え、第 1 の装置と第 2 の装置の他方は、通知手段により通知された情報に対応して認証鍵を生成することを特徴とする。

【0030】請求項 3 に記載の認証システムは、第 1 の装置と第 2 の装置の少なくとも一方は、乱数を生成する乱数生成手段（例えば、図 1 の乱数生成部 23、35）を備え、暗号化手段は、乱数生成手段で生成された乱数を暗号化し、復号化手段は、暗号化された乱数を復号化することを特徴とする。

【0031】請求項 6 に記載の認証装置は、他の装置との間で通信を行う通信手段（例えば、図 1 の通信部 21）と、複数の鍵を記憶する記憶手段（例えば、図 1 のメモリ 11）と、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1 つの認証鍵を生成する生成手段（例えば、図 1 の縮退処理部 13）と、他の装置に対して、他の装置に記憶されている複数の鍵のうちの任意の数の鍵から、対応する 1 つの認証鍵を生成するのに必要な情報と、認証鍵を用いて暗号化するデータを通知する通知手段（例えば、図 1 の通信部 12）と、他の装置が認証鍵を用いて暗号化したデータを、認証鍵を用いて復号化する復号化手段（例えば、図 1 の暗号化部 22）とを備えることを特徴とする。

【0032】請求項 9 に記載の認証装置は、他の装置との間で通信を行う通信手段（例えば、図 1 の通信部 33）と、複数の鍵を記憶する記憶手段（例えば、図 1 のメモリ 31）と、他の装置から通知された情報に基づいて、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、1 つの認証鍵を生成する生成手段（例えば、図 1 の縮退処理部 32）と、他の装置から通知されたデータを、認証鍵を用いて暗号化する暗号化手段（例えば、図 1 の暗号化部 34）とを備えることを特徴とする。

【0033】請求項 12 に記載の認証システムは、第 1 の装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、第 2 の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第 1 の記憶手段（例えば、図 9 のメモリ 11）と、第 1 の記憶手段に記憶されている鍵と、個別データとから、認証鍵



を生成する第1の生成手段（例えば、図9の縮退処理部13）と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段（例えば、図9の制御部24）と、第2の装置との間で通信を行う第1の通信手段（例えば、図9の通信部21）とを備え、第2の装置は、複数の鍵と共通データを記憶する第2の記憶手段（例えば、図9のメモリ31）と、第2の記憶手段に記憶されている複数の鍵のうち、第1の装置の通信手段からの通知に対応するものと、共通データとから、認証鍵を生成する第2の生成手段（例えば、図9の縮退処理部32）と、第1の装置との間で通信を行う第2の通信手段（例えば、図9の通信部33）とを備え、第1の装置と第2の装置の一方は、認証鍵を用いて暗号化を行う暗号化手段（例えば、図9の暗号化部22）を備え、第1の装置と第2の装置の他方は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段（例えば、図9の暗号化部34）を備えることを特徴とする。

【0034】請求項13に記載の認証システムは、認証鍵は、第1の認証鍵と第2の認証鍵で構成され、第1の生成手段は、第1の記憶手段に記憶されている、自己に割り当てられている鍵と、個別データとから、第1の認証鍵を生成し、自己に割り当てられている鍵と、第1の認証鍵を用いて第2の認証鍵を生成し、第2の生成手段は、第2の記憶手段に記憶されている複数の鍵のうち、第1の装置の通知手段からの通知に対応するものと、共通データとから、第1の認証鍵を生成し、第1の認証鍵と、第2の記憶手段に記憶されている複数の鍵のうち、第1の装置の通知手段からの通知に対応するものを用いて第2の認証鍵を生成し、第1の装置と第2の装置は、いずれも暗号化手段と復号化手段を備え、第1の装置と第2の装置の一方は、乱数を生成する乱数生成手段（例えば、図9の乱数生成部23）をさらに備え、第1の装置と第2の装置の一方の暗号化手段は、乱数生成手段で生成された乱数を第1の認証鍵を用いて暗号化し、第1の装置と第2の装置の他方の復号化手段は、第1の装置と第2の装置の一方の暗号化手段により暗号化された乱数を第1の認証鍵を用いて復号化し、第1の装置と第2の装置の他方の暗号化手段は、第1の装置と第2の装置の他方の復号化手段により復号化された乱数を、第2の認証鍵を用いて暗号化し、第1の装置と第2の装置の一方の復号化手段は、第1の装置と第2の装置の他方の暗号化手段により暗号化された乱数を第2の認証鍵を用いて復号化することを特徴とする。

【0035】請求項16に記載の認証システムは、第2の装置は、第1の装置の第1の通信手段から送信を受けた、第1の暗号化データと第2の暗号化データを、鍵識別番号に対応する第1の鍵を用いて復号化する第2の復号化手段（例えば、図18の暗号化部34）と、復号化された第2の鍵と第3の鍵が所定の関係にあるか否かを

判定し、判定結果に対応して第1の鍵を第2の鍵で更新する更新手段（例えば、図18の制御部36）とをさらに備えることを特徴とする。

【0036】請求項18に記載の認証装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶手段（例えば、図9のメモリ11）と、記憶手段に記憶されている鍵と、個別データとから、認証鍵を生成する生成手段（例えば、図9の縮退処理部13）と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段（例えば、図9の制御部24）と、他の装置との間で通信を行う通信手段（例えば、図9の通信部21）と、認証鍵を用いて暗号化を行う暗号化手段（例えば、図9の暗号化部22）とを備えることを特徴とする。

【0037】請求項22に記載の認証装置は、複数の鍵と共通データを記憶する記憶手段（例えば、図9のメモリ31）と、記憶手段に記憶されている複数の鍵のうち、他の装置からの通知に対応するものと、共通データとから、認証鍵を生成する生成手段（例えば、図9の縮退処理部32）と、他の装置との間で通信を行う通信手段（例えば、図9の通信部33）と、他の装置により暗号化されたデータを認証鍵を用いて復号化する復号化手段（例えば、図9の暗号化部34）とを備えることを特徴とする。

【0038】請求項24に記載の認証装置は、他の装置から、記憶手段に記憶されている複数の鍵のうち、所定の第1の鍵を新たな第2の鍵で更新するために、第2の鍵を第1の鍵で暗号化した第1の暗号化データと、第2の鍵に対して所定の関係にある第3の鍵を、第1の鍵で暗号化した第2の暗号化データを、更新する鍵の鍵識別番号とともに送信を受けたとき、第1の暗号化データと第2の暗号化データを、更新する鍵の鍵識別番号に対応する第1の鍵を用いて復号化する第2の復号化手段（例えば、図18の暗号化部34）と、復号化された第2の鍵と第3の鍵が所定の関係にあるか否かを判定し、判定結果に対応して第1の鍵を第2の鍵で更新する更新手段（例えば、図18の制御部36）とをさらに備えることを特徴とする。

【0039】図1は、本発明の認証システムの構成例を示している。この構成例においては、システムが、コントローラ1、リーダライタ2、およびICカード3により構成されている。ICカード3は、各ユーザが、例えば定期券などの代わりに所持するものであり、リーダライタには、このICカード3を利用する鉄道会社の改札口に設けられているものである。なお、本明細書において、システム用語は、複数の装置で構成されている全体の装置を総称して使用する場合に、適宜用いる。

【0040】コントローラ1は、メモリ11を有し、ここにICカード3のメモリ31の各エリアにアクセスす

るのに必要な暗号鍵と、それに対応するプロバイダ番号を記憶している。通信部12は、リーダライタ2の通信部21との間で有線または無線で、通信を行う。縮退処理部13は、メモリ11に記憶されている複数の暗号鍵の中から、所定の数の暗号鍵を読み出し、1つの縮退鍵を生成する処理を行う。制御部14は、コントローラ1の各部の動作を制御する他、認証処理を行うようになされている。

【0041】リーダライタ2の通信部21は、有線または無線で、コントローラ1の通信部12、またはICカード3の通信部33と通信を行うようになされている。暗号化部22は、乱数生成部23で生成した乱数を暗号化するとともに、ICカード3から伝送されてきた暗号化されている乱数を復号化する処理を行う。制御部24は、リーダライタ2の各部の動作を制御するとともに、認証処理を行うようになされている。

【0042】ICカード3は、メモリ31を有し、このメモリ31は、複数のエリア（図1の例の場合、5個のエリア）に区分されている。各エリアには、各プロバイダ（例えば各鉄道会社）が個別にアクセスし、適宜データを書き込み、または読み出すようになされている。ただし、各エリア毎に異なる暗号鍵が対応付けされており、所定のエリアiにアクセスするには、対応する暗号鍵iが必要となる。

【0043】縮退処理部32は、複数の暗号鍵を縮退処理し、1つの縮退鍵を生成する処理を行う。暗号化部34は、乱数生成部35で生成した乱数を暗号化する処理を行うとともに、リーダライタ2より供給されてきた、暗号化されているデータを復号化する処理を行う。制御部36は、ICカード3の各部の動作を制御するとともに、認証処理を行うようになされている。

【0044】図2は、ICカード3のメモリ31のデータ構造のより詳細な例を表している。この例においては、エリア51は共通領域とされ、各プロバイダに共通のデータが記憶されるようになされている。また、エリア52は、個々のプロバイダ専用の領域とされ、個々の対応するプロバイダのみが、その領域にアクセスすることができるようになされている。

【0045】エリア53は、エリア51とエリア52を管理するのに必要な情報が記録されるようになされている。その情報とは、この例の場合、個々のプロバイダに割り付けられているプロバイダ番号、そのプロバイダに対して割り付けられている領域を示すブロック割り付け情報、読み出しのみ可能、書き込みのみ可能、読み出しと書き込みの両方が可能といった許可情報、暗証鍵、および暗証鍵のバージョンとされている。

【0046】例えば、プロバイダ番号00は、各プロバイダ共通のものとされ、そのブロック割り付け情報には、共通領域としてのエリア51のアドレスが書き込まれている。また、その許可情報としては、共通領域とし

てのエリア51に対してアクセス可能な情報が規定されている。さらに、その暗号鍵とそのバージョンとしては、共通領域としてのエリア51に対してアクセスするのに必要な暗号鍵と、そのバージョンが規定されている。

【0047】エリア54は、システムIDブロックとされ、このICカード3を適用するシステムのIDが書き込まれる。

【0048】なお、コントローラ1のメモリ11には、この図2に示す、プロバイダ番号、許可情報、暗号鍵バージョン、および暗号鍵が記憶されている。

【0049】図3は、縮退処理部13（または縮退処理部32）の構成例を示している。ただし、この処理は、実際には、ソフトウェアにより行われる。

【0050】すなわち、縮退処理部13または32においては、ICカード3にn個の暗号鍵が存在する場合、2入力縮退回路81-1乃至81-(n-1)の(n-1)個の回路が設けられており、それぞれに2つのデータが入力され、1つのデータを出力するようになされている。2入力縮退回路81-1には、プロバイダ1（鉄道会社1）の暗号鍵とプロバイダ2（鉄道会社2）の暗号鍵が入力されている。2入力縮退回路81-1は、この2つの暗号鍵から1つの縮退鍵を生成し、後段の2入力縮退回路81-2に供給する。2入力縮退回路81-2は、2入力縮退回路81-1より入力された縮退鍵と、プロバイダ3（鉄道会社3）の暗号鍵を縮退処理して、後段の2入力縮退回路81-3（図示せず）に出力する。以下、同様の処理が、各2入力縮退回路81-iにおいて行われ、最後の2入力縮退回路81-(n-1)で生成された縮退鍵が、最終的な1つの縮退鍵とされる。

【0051】なお、n=1の場合（暗号鍵が1個の場合）、入力された暗号鍵が、そのまま縮退鍵として出力される。

【0052】図4乃至図6は、図3に示した2入力縮退回路81-iの構成例を表している。図4の暗号化回路81-iは、前段からの入力を、予め用意されている暗号鍵に対応して暗号化し、後段に出力するようになされている。例えば、2入力縮退回路81-1を、この暗号化回路81-iで構成する場合、プロバイダ1の暗号鍵がデータとして入力され、プロバイダ2の暗号鍵が暗号鍵として入力される。そしてプロバイダ2の暗号鍵を用いて、プロバイダ1の暗号鍵（データ）を暗号化して、2入力縮退回路81-2に出力する。

【0053】図5の暗号化回路81-iは、前段からの入力を暗号鍵として受け取り、予め用意されている暗号鍵をデータとして受け取り、暗号化処理を行って、後段に出力する。例えば、この暗号化回路81-iを、図3の2入力縮退回路81-1に応用すると、プロバイダ2の暗号鍵がデータとして入力され、プロバイダ1の暗号

鍵が暗号鍵として入力される。そして、プロバイダ2の暗号鍵をプロバイダ1の暗号鍵を利用して暗号化し、縮退鍵として、後段の2入力縮退回路81-2に出力する。

【0054】なお、図4と図5に示す暗号化方法としては、例えば、DES(Data Encryption Standard)、FEAL(Fast Data Encipherment Algorithm)などを用いることができる。

【0055】図6では、暗号化回路81-iが、排他的論理和回路(XOR)により構成されている。例えば、この暗号化回路81-iを、図3の2入力縮退回路81-1に応用すると、プロバイダ1の暗号鍵とプロバイダ2の暗号鍵の排他的論理和が演算され、その演算結果が、縮退鍵として、後段の2入力縮退回路81-2に出力されることになる。

【0056】図3において、各プロバイダの暗号鍵は、例えば、30バイトで表されるデジタルデータのうちの1つとされる、この場合、縮退鍵も同一のバイト数のデジタルデータとなる。暗号鍵は、30バイトで規定される数字の中の1つであるから、すべての組み合わせの中から所定の1つの数字を選択し、順番にテストして行けば、暗号鍵を見破ることは、理論的には可能である。しかしながら、その演算を行うのには、膨大な時間がかかり、30バイトで表される数字のどれが、実際の暗号鍵であるのかを調べるのは実質的には不可能である。

【0057】次に、図7のタイミングチャートを参照して、その動作について説明する。なお、コントローラ1とリーダライタ2は、ここでは別の装置として示されているが、一体的な装置とすることも可能である。

【0058】コントローラ1の制御部14は、ステップS1において、通信部12を制御し、リーダライタ2に対して充分短い周期(ICカード3を所持するユーザが、鉄道駅の改札口を通過するのを検知できる周期)でポーリングを指令する。リーダライタ2の制御部24は、通信部21を介してこの指令を受けたとき、ステップS2において、通信部21を制御し、ICカード3に対するポーリングを実行する。ICカード3の制御部36は、通信部33を介してリーダライタ2の通信部21からポーリングの指令を受けたとき、ステップS3において、自己の存在を通知する。リーダライタ2の制御部24は、通信部21を介して、ICカード3からこの通知を受けたとき、ステップS4において、ICカード3の存在をコントローラ1に通知する。

【0059】コントローラ1の制御部14は、通信部12を介してこの通知を受けたとき、ステップS5で縮退処理部13を制御し、ICカード3のメモリ31のうち、アクセスすべきエリアの暗号鍵をメモリ11から読み出させる。例えば、図1の例においては、エリア1、エリア2、およびエリア4にアクセスするため、暗号鍵

1、暗号鍵2、および暗号鍵4が、縮退処理部13に呼び出されている。縮退処理部13は、この3つの暗号鍵を用いて縮退処理を行う。すなわち、図3に示したように、2入力縮退回路81-1において、暗号鍵1を暗号鍵2で暗号化し、2入力縮退回路81-2に出力する。2入力縮退回路81-2は、2入力縮退回路81-1より供給された暗号鍵1と暗号鍵2を縮退した結果得られた縮退鍵を、暗号鍵3で暗号化する。そして、得られた縮退鍵が、最終的な縮退鍵とされる。

【0060】制御部14は、このように1つの縮退鍵が生成されると、これをプロバイダ番号(鍵の番号)とプロバイダの数(鍵の数)、および縮退処理の順序とともに、ステップS6において、リーダライタ2に通知させる。リーダライタ2の制御部24は、通信部21を介してコントローラ1の通信部12から、この情報の入力を受けたとき、ステップS7において、乱数生成部23に、乱数r1を生成させる。制御部24はこの乱数r1を、ステップS8で通信部21からICカード3に、通知させる。このとき、制御部24は、コントローラ1から提供を受けたプロバイダ数とプロバイダ番号も、合わせてICカード3に通知する。

【0061】ICカード3の制御部36は、このような通知を受けたとき、ステップS9で、まず縮退鍵生成処理を実行する。すなわち、制御部36は、リーダライタ2から転送されてきたプロバイダ番号(鍵番号)に対応する暗号鍵をメモリ31から読み出し、これを縮退処理部32に供給し、縮退処理を実行させる。図1の例の場合、暗号鍵1、暗号鍵2、および暗号鍵4に対応するプロバイダ番号が転送されてくるので、縮退処理部32は、これらのプロバイダ番号に対応する暗号鍵1、暗号鍵2、および暗号鍵4をメモリ31から読み出し、縮退処理部32に供給する。縮退処理部32は、これらの3つの暗号鍵を、指定された順序(例えば、入力されたプロバイダの順序)で縮退処理し、最終的に1つの縮退鍵を生成する。これにより、コントローラ1が、ステップS5で生成した縮退鍵と同一の縮退鍵が、ICカード3において生成されたことになる。

【0062】次に、ステップS10で、制御部36は、リーダライタ2から通知を受けた乱数r1と、縮退処理部32で生成された縮退鍵を暗号化部34に出力し、乱数r1を縮退鍵で暗号化させる。そして、暗号化した乱数R1を生成させる。

【0063】次に、ステップS11において、制御部36は、乱数生成部35で、所定の乱数r2を生成させる。そして、ステップS12において、制御部36は、通信部33を制御し、ステップS10で、暗号化した乱数R1と、ステップS11で生成した乱数r2をリーダライタ2に転送させる。

【0064】リーダライタ2の制御部24は、通信部21を介して、乱数r2と暗号化された乱数R1の供給を

受けたとき、ステップS 1 3で、暗号化部 2 2を制御し、暗号化されている乱数R 1をコントローラ 1より供給を受けた縮退鍵を利用して復号化させる。制御部 2 4は、復号化した結果得られた乱数が、ステップS 7で生成した乱数r 1と等しいか否かをさらにチェックし、等しくない場合、I Cカード3は適正なI Cカードではないとして、ステップS 1 4において、コントローラ 1に対して、その旨を通知する。このとき、コントローラ 1はエラー処理を実行する（例えば、ユーザの改札口の通過を禁止する）。

【0065】これに対して、ステップS 1 3において、復号化された乱数と乱数r 1が等しいと判定された場合、ステップS 1 5に進み、制御部 2 4は、暗号化部 2 2を制御し、I Cカード3より供給を受けた乱数r 2を、コントローラ 1より供給を受けた縮退鍵を用いて暗号化させ、暗号化された乱数R 2を生成させる。さらに、制御部 2 4は、このようにして生成した、暗号化した乱数R 2を、ステップS 1 6で、I Cカード3に転送させる。

【0066】I Cカード3の制御部 3 6は、このように暗号化された乱数R 2の供給を受けたとき、ステップS 1 7で、暗号化部 3 4を制御し、暗号化されている乱数R 2を、ステップS 9で生成した縮退鍵を用いて復号化させる。そして、復号化された乱数が、ステップS 1 1で生成した乱数r 2と等しいか否かを判定する。そして、判定した結果を、ステップS 1 8で、通信部 3 3を介してリーダライタ 2に転送させる。

【0067】リーダライタ 2の制御部 2 4は、I Cカード3から認証結果の通知を受けたとき、ステップS 1 9で、これをさらに通信部 2 1からコントローラ 1通知する。

【0068】コントローラ 1の制御部 1 4は、通信部 1 2を介して、この通知を受けたとき、この通知がNGであるとされている場合には、エラー処理を実行する。これに対してOKであるとされている場合（I Cカード3が適正なものである場合）には、ステップS 2 0において、読み出しまたは書き込みなどの必要なコマンドをリーダライタ 2に出力する。リーダライタ 2は、このコマンドの転送を受けたとき、ステップS 2 1で、さらにI Cカード3に対して、読み出しまたは書き込みの指令を出力する。いまの場合、このようにして、I Cカード3のエリア 1、エリア 2、およびエリア 4の読み出しまたは書き込みが指令される。

【0069】その結果、I Cカード3の制御部 3 6は、エリア 1、エリア 2、またはエリア 4に書き込みが指令されている場合には、書き込み処理を実行する。そして、読み出しが指令されている場合には、読み出し処理を実行する。読み出されたデータは、ステップS 2 2で、I Cカード3からリーダライタ 2に転送され、さらに、リーダライタ 2からコントローラ 1に、ステップS

2 3で転送される。

【0070】以上のように、複数のエリアにアクセスする場合に、個々に必要となる暗証鍵を個々に認証するのではなく（例えば図 1 の例の場合、暗号鍵 1、暗号鍵 2、暗号鍵 4について、個々に認証処理を行う（すなわち、合計 3 回の認証処理を行う）のではなく）、複数の暗証鍵から 1 つの縮退鍵を生成し、この 1 つの縮退鍵で 1 回だけ認証処理を行うようにしたので、迅速な認証処理が可能となる。

10 【0071】なお、縮退鍵は、暗号鍵と同一のバイト数（長さ）としたが、異なるバイト数とすることも可能である。ただし、この縮退鍵は、認証に用いるだけなので、その縮退鍵から元の複数の暗号鍵を復元することが可能である必要はない。

【0072】図 8 は、縮退鍵を生成する他の方法を表している。この例においては、プロバイダ 1 乃至プロバイダ n それぞれに、暗号鍵 K 1 乃至 K n が割り当てられる他、最初の 2 入力縮退回路 8 1 - 1 に、予め含められた秘密（各プロバイダに共通のデータとされるので、必ずしも秘密でなくともよいが）のデータ D 0 が入力され、2 入力縮退回路 8 1 - 1 は、このデータ D 0 を、プロバイダ 1 の暗号鍵 K 1 に基づいて暗号化するようになされている。そして、2 入力縮退回路 8 1 - 2 が、2 入力縮退回路 8 1 - 1 の出力 D 1 を、プロバイダ 2 の暗号鍵 K 2 に基づいて暗号化するようになされている。以下、順次、同様の処理が、2 入力縮退回路 8 1 - i において行われ、最終段の 2 入力縮退回路 8 1 - n の出力が最終的な縮退鍵とされる。

30 【0073】図 3 に示すように縮退鍵を生成する場合、プロバイダ 2 は、プロバイダ 1 の暗号鍵を知らないと、縮退鍵を生成することができない。基本的に、各プロバイダは独立しているので、所定のプロバイダの暗号鍵を他のプロバイダに知らせるようにすることは、秘密性を確保する上で好ましいことではない。

【0074】これに対して、図 8 に示すように縮退鍵を生成すると、自分自身の暗号鍵を他のプロバイダに通知しなくても、他のプロバイダは、縮退鍵を生成することができる。

40 【0075】図 9 乃至図 1 1 は、図 8 に示すように、縮退鍵を生成する場合のプロバイダ 1、プロバイダ 2、またはプロバイダ 4 の、コントローラ 1 およびリーダライタ 2 と、I Cカード 3 の構成例を表している。

【0076】これらの図に示すように、I Cカード 3 には、メモリ 3 1 に、エリア 1 乃至エリア 5 に対応する暗号鍵 K 1 乃至暗号鍵 K 5 の他、所定のデータ（共通データ）D 0 が予め記憶されている。

50 【0077】そして、プロバイダ 1 のメモリ 1 1 には、自分自身の暗号鍵 K 1 とデータ D 0 2 4 が記憶されており（図 9）、プロバイダ 2 のメモリ 1 1 には、自分自身の暗号鍵 K 2 とデータ D 0 1 4 が記憶されており（図 1

0)、プロバイダ4のメモリ11には、自分自身の暗号鍵K4とデータD012が記憶されている(図11)。

【0078】これらのデータ(個別データ)D024, D014, D012は、図12乃至図14に示す方法で生成されたものである。

【0079】すなわち、プロバイダ1は、データD024を得るために、予め定めたデータD0を、プロバイダ2により、その暗号鍵K2を用いて、2入力縮退回路81-1で縮退して、データD02を生成してもらう。そして、このデータD02をプロバイダ4に提供して、その暗号鍵K4で2入力縮退回路81-2で縮退して、データD024を生成してもらう。プロバイダ1は、このデータD024をプロバイダ4から提供を受け、メモリ11に記憶させる。

【0080】なお、この場合、データD0を先にプロバイダ4に提供し、暗号鍵K4で縮退して、データD04を生成してもらい、このデータD04をプロバイダ2に提供して、暗号鍵K2で縮退して、データD042を生成してもらい、これをメモリ11に記憶させるようにしてもよい。そこで、プロバイダ1は、いずれの順序で縮退を行ったのかを示す縮退の順番もメモリ11に記憶しておく。

【0081】また、図13に示すように、プロバイダ2は、プロバイダ1に依頼して、その暗号鍵K1でデータD0を縮退したデータD01を生成してもらう。そして、このデータD01をプロバイダ4に提供して、暗号鍵K4で縮退してもらい、データD014を生成してもらう。そして、このデータD014をメモリ11に記憶させる。なお、この場合も、先にプロバイダ4に縮退処理を依頼して、暗号鍵K4を用いて生成されたデータD04をプロバイダ1に提供し、これをさらに暗号鍵K1を用いて縮退してもらい、データD041を得て、これをメモリ11に記憶させるようにしてもよい。プロバイダ2は、縮退の順番もメモリ11に記憶させる。

【0082】さらに、図14に示すように、プロバイダ4は、プロバイダ1に依頼して、データD0を暗号鍵K1を用いて縮退し、データD01を生成してもらう。そして、このデータD01をプロバイダ2に提供して、暗号鍵K2を用いて縮退し、データD012を生成してもらう。このデータD012をメモリ11に記憶させる。この場合も同様に、先にプロバイダ2にデータD0を暗号鍵K2を用いて縮退し、データD02を生成し、このデータD02をプロバイダ1により暗号鍵K1を用いて縮退し、データD021を生成してもらうようにしてもよい。プロバイダ4も、縮退の順序をメモリ11に記憶させておく。

【0083】各プロバイダは、次のように認証処理を行うことができる。例えば、プロバイダ1においては、図9に示すように、制御部14が縮退処理部13を制御し、メモリ11からデータD024と暗号鍵K1を読み

出し、縮退鍵を生成させる。この縮退鍵は、リーダライタ2に転送される。このとき、リーダライタ2には、プロバイダの数(この例の場合、3)、プロバイダ番号(いまの場合、プロバイダ1、プロバイダ2、およびプロバイダ4)、並びに、縮退の順序(いまの場合、プロバイダ2、プロバイダ4、プロバイダ1の順)を通知する。制御部24は、通信部21を制御し、コントローラ1の制御部14から転送されてきたこれらのプロバイダ数、プロバイダ番号、および縮退順序の情報を、ICカード3に通知する。

【0084】ICカード3においては、通信部33でこれらの情報を受信すると、制御部36は、これらの情報に対応して縮退処理部32を制御し、縮退鍵を生成させる。縮退処理部32は、メモリ31からデータD0を読み出し、これを指定された順序と指定されたプロバイダの番号の暗号鍵を用いて、順次縮退する。すなわち、データD0を暗号鍵K2を用いて縮退し、データD02を得る。このデータD02を暗号鍵K4を用いて縮退し、データD024を得る。さらに、このデータD024を暗号鍵K1を用いて、縮退鍵を生成する。このようにして生成された縮退鍵は、コントローラ1の縮退処理部13が生成した縮退鍵と同一の縮退鍵となっている。

【0085】従って、以下、図7を参照して説明した場合と同様に、ステップS10以降の処理を行って、認証処理を行うことができる。そして、プロバイダ1のリーダライタ2は、ICカード3のメモリ31のエリア1、エリア2、およびエリア4にアクセスすることが可能となる。

【0086】一方、プロバイダ2においては、図10に示すように、制御部14は、縮退処理部13を制御し、メモリ11からデータD014を読み出し、これを、やはりメモリ11から読み出した暗号鍵K2を用いて縮退させる。そして、生成した縮退鍵をリーダライタ2に転送する。このとき、リーダライタ2には、プロバイダ数(いまの場合、3)、プロバイダ番号(いまの場合、プロバイダ1、プロバイダ2、およびプロバイダ4)、および縮退処理の順番(いまの場合、プロバイダ1、プロバイダ4、プロバイダ2の順番)が、リーダライタ2に通知される。

【0087】リーダライタ2は、これらの情報をICカード3に転送する。ICカード3においては、これらの情報に対応して、縮退鍵が生成される。

【0088】すなわち、ICカード3の縮退処理部32は、メモリ31から、データD0を読み出し、これを最初に暗号鍵K1を用いて縮退し、データD01を得る。そして、このデータD01がさらに暗号鍵K4を用いて縮退され、データD014が生成される。このデータD014は、さらに暗号鍵K2を用いて縮退される。このようにして生成された縮退鍵は、コントローラ1において生成された縮退鍵と同一の縮退鍵となっている。従っ

て、プロバイダ2のリーダライタ2は、ICカード3のメモリ31のエリア1、エリア2、およびエリア4に対してアクセスすることができる。

【0089】さらに、図11に示すように、プロバイダ4においても、コントローラ1の制御部14が縮退処理部13を制御し、メモリ11に記憶されているデータD012を暗号鍵K4を用いて縮退鍵を生成し、これをリーダライタ2に転送する。このとき、プロバイダ数（いまの場合、3）、プロバイダ番号（いまの場合、プロバイダ1、プロバイダ2、およびプロバイダ4）、および縮退順序（いまの場合、プロバイダ1、プロバイダ2、プロバイダ4の順番）が通知される。これらの情報は、ICカード3に転送される。ICカード3は、これらの情報に基づいて、縮退処理を実行する。

【0090】すなわち、縮退処理部32は、メモリ31からデータD0を読み出し、これを暗号鍵K1を用いてデータD01を生成する。次に、このデータD01を暗号鍵K2を用いて縮退し、データD012を生成する。そして、このデータD012が、さらに暗号鍵K4を用いて縮退され、最終的な縮退鍵が生成される。このようにして生成された縮退鍵は、コントローラ1において生成された縮退鍵と同一となっている。従って、リーダライタ2は、ICカード3のメモリ31のエリア1、エリア2、およびエリア4に対してアクセスすることができる。

【0091】図15は、さらに他の縮退鍵生成の方法を表している。この方法においては、最終的な縮退鍵を生成する2入力縮退回路81-nに入力されるデータDn-1と、ICカード3が予め保持しているID番号とを演算して、その演算結果に対して暗号鍵Knを用いて縮退鍵を生成するようにしている。その他の処理は、図8における場合と同様である。

【0092】図16は、図15に示す方法に従って、縮退鍵を生成する場合のコントローラ1、リーダライタ2、およびICカード3の構成例を表している。なお、この構成は、プロバイダ4の構成を表している。同図に示すように、コントローラ1のメモリ11は、データD012と暗号鍵K4、並びに縮退順序を記憶している。リーダライタ2は、通信部21が受信したデータからIDを取得するID取得部211を有している。また、ICカード3は、メモリ201（メモリ31と同一のメモリとすることもできる）に、ICカード3に固有のID番号が予め記憶されている。

【0093】このように、ID番号を用いて認証処理を行うようにすると、同一のプロバイダの組み合わせ（例えばプロバイダ1、プロバイダ2、およびプロバイダ4の組み合わせ）のICカードを所持している複数のユーザが、近接した状態で、所定のプロバイダの改札口を通過するような場合の混乱を避けることができる。

【0094】すなわち、複数のICカード3が所定のプ

ロバイダのリーダライタ2の近傍を通過するとき、リーダライタ2からの要求に対して、複数のICカード3がそれぞれ応答することになり、リーダライタ2がいずれのICカードからの応答であるのかを判別することができず、誤った処理が行われるおそれがある。これに対して、ID番号を用いると、このような混乱を避けることができる。

【0095】例えば、図17に示すように、ICカード3AとICカード3Bが、リーダライタ2の近傍を通過しようとするとき、リーダライタ2が、ステップS41において、ICカード3に対してIDを要求する。この要求は、ICカード3Aの通信部33だけでなく、ICカード3Bの通信部33でも受信される。ICカード3Aの制御部36は、このようにしてID要求信号を受信すると、ステップS42において、乱数生成部35を制御し、所定の乱数を発生させる。そして、ステップS43において、発生された乱数に対応するタイムスロットの割当処理を実行する。すなわち、リーダライタ2とICカード3の間の通信は、時分割多重動作で行われ、ICカード3Aは、その複数のタイムスロットのうち、発生された乱数に対応するタイムスロットを、自己の通信のタイムスロットとして割り当てる。そして、割り当てたタイムスロットのタイミングにおいて、ICカード3Aの制御部36がメモリ201から読み出したID番号（ID<sub>A</sub>）を、通信部33を介して、ステップS44でリーダライタ2に送信させる。

【0096】同様の処理が、他のICカード3Bにおいても実行される。すなわち、ICカード3Bの制御部36は、リーダライタ2からID要求信号を受信すると、ステップS45で乱数生成部35を制御し、乱数を発生させる。そして、ステップS46において、生成された乱数に対応するタイムスロットを、自己のタイムスロットとして割り当てる。ステップS47において、メモリ201に記憶されているID番号（ID<sub>B</sub>）を読み出し、割り当てられたタイムスロットのタイミングで、リーダライタ2に転送する。

【0097】リーダライタ2においては、ICカード3A、3Bから送信されてきたID番号を通信部21で受信すると、これをID取得部211に供給し、記憶させる。そして、ステップS48において、制御部24は、乱数生成部23を制御し、乱数r1を生成させる。さらに、ステップS49において、制御部24は、取得したIDのうち、例えば先に取得した方を選択する。制御部24は、さらに、コントローラ1のメモリ11から、データD012、暗号鍵K4、および縮退順序の情報の提供を受ける。そして、これらの情報に対応して、縮退鍵を生成する。

【0098】最初に、制御部24は、データD012に、この選択したID（例えば、ICカード3のID<sub>A</sub>）に対して、所定の演算を施す。この演算は、加

算、排他的論理和の演算などとして行うことができる。制御部24は、この演算結果を暗号鍵K4を用いて縮退し、縮退鍵を生成する。

【0099】さらに、ステップS50において、プロバイダ数、プロバイダ番号、縮退順序、および乱数 $r_1$ が、ICカード3に送信される。この情報は、ICカード3Aと、ICカード3Bの両方において受信される。ICカード3Bは、この情報を受信したとき、ステップS51で、指定された順序に従って、データD0を暗号鍵K1で縮退し、データD01を得、これを暗号鍵K2で縮退して、データD012を得る。そして、さらに、メモリ201からID<sub>h</sub>を読み取り、データD012と演算した結果を、暗号鍵K4で縮退する。

【0100】このようにして生成した縮退鍵を用いて、暗号化部34が、暗号化されている乱数 $r_1$ を復号化する。しかしながら、この乱数 $r_1$ は、ID<sub>h</sub>を用いて生成した縮退鍵で暗号化されているため、ID<sub>h</sub>を用いて生成した縮退鍵では復号化することができない。従って、ICカード3Bは、以後、リーダライタ2からの送信に対して応答しない。

【0101】これに対して、ICカード3Aにおいては、ステップS52で、制御部36が、リーダライタ2から転送されてきた情報に対応して、縮退鍵を生成する。すなわち、指定された縮退順序に従って、ICカード3Aの縮退処理部32は、最初にメモリ31から読み出したデータD0を、エリア1から読み出した暗号鍵K1を用いて縮退し、データD01を生成する。そして、このデータD01をエリア2から読み出した暗号鍵K2を用いて縮退し、データD012を生成する。さらに、このデータD012とメモリ201から読み出したID番号(ID<sub>h</sub>)とに対して所定の演算を施し、その演算結果に対して、メモリ31のエリア4から読み出した暗号鍵K4を用いて縮退処理を行い、縮退鍵を生成する。このようにして生成した縮退鍵は、リーダライタ2がステップS49で生成した縮退鍵と同一の縮退鍵となる。

【0102】従って、以後、ステップS53乃至ステップS59に示す、図7におけるステップS10乃至ステップS17に対応する処理を実行して、認証処理を行うことができる。その処理は、図7において説明した場合と同様であるので、その説明は省略する。

【0103】図18は、暗号鍵を変更する方法を表している。例えば、プロバイダ1がその暗号鍵K1を変更しようとする場合、所定の乱数 $e_1$ を発生し、これを新たな鍵K1'とする。このように、自分自身の暗号鍵を変更したとき、プロバイダ1は、自分自身のリーダライタ2を利用するユーザのICカード3のメモリ31に記憶されているエリア1の暗号鍵K1は、適宜自分でこれを更新することができる。しかしながら、他のプロバイダ2、またはプロバイダ4のリーダライタ2を使用するユーザのICカード3の暗号鍵K1も更新する必要があ

る。この場合、プロバイダ1は、他のプロバイダ2またはプロバイダ4に対して、新たな暗号鍵K1'を教えずに、暗号鍵K1を新たな暗号鍵K1'に更新させることができる。

【0104】この場合、プロバイダ1は、最初に次式を演算して、データC1、C2を生成する。

$$C1 = E(e1, K1)$$

$$C2 = E(e2, K1)$$

【0105】なお、ここで、E(A, B)は、データAを鍵Bを用いて暗号化することを意味する。暗号化の方法としては、DES, FEALなどを用いることができる。

【0106】また、 $e_2$ は、次式を満足する値である。  

$$e1 + e2 = F$$

【0107】なお、この値Fは、予め定められている値であり、他のプロバイダ2、プロバイダ4も、自分自身の暗号鍵を変更する場合に用いるものとして知っている値であり、ICカード3にも、メモリ31に予め記憶されている。

【0108】プロバイダ1は、このようにして、データC1、C2を生成すると、この値を、自分自身の暗号鍵K1に割り当てられている鍵番号(いまの場合、鍵番号1)とともに、他のプロバイダに通知する。各プロバイダは、これらのデータを用いて、そのリーダライタ2を使用するICカード3のメモリ31内の鍵K1を、次のようにして更新する。この更新処理について、プロバイダ4を例として次に説明する。

【0109】すなわち、プロバイダ4のリーダライタ2は、ICカード3に対して、データC1、C2を送信する。ICカード3の暗号化部34は、次式を演算して、 $e_1$ 、 $e_2$ を求める。

$$e1 = D(C1, K1)$$

$$e2 = D(C2, K1)$$

【0110】なお、ここで、D(A, B)は、データAを鍵Bを用いて復号化することを意味する。

【0111】すなわち、ICカード3は、メモリ31に記憶されている鍵K1を用いて、データC1、C2を復号化し、データ $e_1$ 、 $e_2$ を得ることができる。

【0112】制御部36は、さらに、以上のようにして得た $e_1$ と $e_2$ を加算し、その加算結果がメモリ31に予め記憶されている所定の値Fと等しいか否かを判定する。等しい場合には、データC1を復号して得られるデータ $e_1$ を、鍵K1に代わる新たな鍵K1'として更新する。

【0113】これに対して、 $e_1$ と $e_2$ の和がFと異なる場合、不正な更新の要求であるとして、更新処理を行わないようにする。

【0114】例えば、悪意を持ったプロバイダが、プロバイダ1の暗号鍵K1を改ざんしようとして、次式を演算して、 $e_1'$ 、 $e_2'$ を得たとする。



$e1' = D(C1', K1)$

$e2' = D(C2', K1)$

【0115】この $C1'$ 、 $C2'$ は、改ざんを試みたプロバイダが適当に設定した値である。

【0116】しかしながら、このようにして生成された $e1'$ と $e2'$ を加算しても、その加算結果は、一般的には、値Fには等しくならない。この値Fになる $e1'$ 、 $e2'$ の組み合わせを発見するには、相当の時間を必要とし、実質的には極めて困難である。従って、第3者が、他人の暗号鍵を改ざんすることが防止される。

【0117】なお、プロバイダ2も同様の処理を行って、そのリーダライタ2を利用するICカード3のメモリ31の暗号鍵K1を更新する。

【0118】なお、以上のようにして、プロバイダ1の暗号鍵K1が変更された場合、プロバイダ1、プロバイダ2、およびプロバイダ4は、図12乃至図14を参照して説明した場合と同様の処理を再び行い、それぞれに記憶するデータD024、D014、D012を更新する。

【0119】図19は、認証処理のさらに他の方法を示している。なお、この図19のリーダライタ2は、プロバイダ4のリーダライタを表している。

【0120】この例においては、制御部24が、メモリ11に記憶されている暗号鍵K4とデータD012を用いて、縮退鍵Ksを生成する。そして、制御部24は、例えば、暗号鍵K4の偶数ビットと縮退鍵Ksの奇数ビットとを合成し、第1の縮退鍵 $K_{s1}$ を生成し、暗号鍵K4の奇数ビットと縮退鍵Ksの偶数ビットとを合成し、第2の縮退鍵 $K_{s2}$ を生成する。

【0121】第1の縮退鍵 $K_{s1}$ は、暗号化部22の暗号化部22Aに入力され、乱数生成部23で生成された乱数を暗号化するのに用いられる。この暗号化された乱数は、ICカード3に送信される。また、このとき、上述した場合と同様にして、縮退鍵を生成するのに必要な情報が、同時にICカード3に送信される。

【0122】ICカード3は、この情報を用いて、メモリ31からデータD0を読み出し、さらに暗号鍵K1、K2、K4を順次適用して、縮退鍵Ksを生成する。この縮退鍵Ksは、リーダライタ2が生成した縮退鍵Ksと同一の値となっている。

【0123】制御部36は、リーダライタ2と同様の処理を行うことで、第1の縮退鍵 $K_{s1}$ と第2の縮退鍵 $K_{s2}$ を生成する。

【0124】そして、暗号化部34の復号化部34Bは、リーダライタ2より送信されてきた暗号化されている乱数を復号化し、この復号化した乱数を暗号化部34Aに転送する。暗号化部34Aにおいては、第2の縮退鍵 $K_{s2}$ を用いて暗号化し、リーダライタ2に送信する。

【0125】リーダライタ2においては、暗号化部22

の復号化部22Bで、ICカード3より送信されてきた暗号化されている乱数を、第2の縮退鍵 $K_{s2}$ を用いて復号化する。復号結果は、制御部24に転送される。

【0126】このようにして復号された乱数は、ICカード3が適正なものであれば、乱数生成部23で生成した乱数と同一の乱数となっている。従って、この受信した乱数が生成した乱数と等しいか否かを調べることで、認証処理を行うことができる。

【0127】

【発明の効果】以上の如く、請求項1に記載の認証システムおよび請求項5に記載の認証方法によれば、複数の鍵から1つの認証鍵を生成し、この認証鍵を用いて、暗号化と復号化を行うようにしたので、より迅速な認証を行うことが可能なシステムを実現することができる。

【0128】請求項6に記載の認証装置および請求項8に記載の認証方法によれば、他の装置に対して認証鍵を生成するのに必要な情報を通知し、他の装置が、その情報に基づいて生成した認証鍵を用いて、暗号化したデータを復号化するようにしたので、他の装置との間において、迅速な認証処理が可能となる。

【0129】請求項9に記載の認証装置および請求項11に記載の認証方法によれば、他の装置から通知された情報に基づいて、1つの認証鍵を生成し、やはり他の装置から通知されたデータを、その認証鍵を用いて、暗号化するようにしたので、他の装置との間で、迅速な認証処理が可能となる装置を提供することが可能となる。

【0130】請求項12に記載の認証システムおよび請求項17に記載の認証方法によれば、第1の装置で、自己に割り当てられた鍵と、個別データとから、認証鍵を生成し、第2の装置で、第1の装置からの通知と、共通データとから、認証鍵を生成するようにしたので、より秘密性を保持しつつ、他の装置との間において、迅速な認証処理が可能となる。

【0131】請求項18に記載の認証装置および請求項21に記載の認証方法によれば、自己に割り当てられた鍵と、個別データとから、認証鍵を生成するようにしたので、秘密性を確保しつつ、他の装置との間において、迅速な認証処理が可能となる。

【0132】請求項22に記載の認証装置および請求項25に記載の認証方法によれば、他の装置からの通知に対応する鍵と、共通データとから、認証鍵を生成するようにしたので、秘密性を確保しつつ、他の装置との間において、迅速な認証処理が可能となる。

【図面の簡単な説明】

【図1】本発明の認証システムの構成例を示すブロック図である。

【図2】図1のメモリ31のデータ構造の例を示す図である。

【図3】図1の縮退処理部13の構成例を示す図である。

【図4】図3の2入力縮退回路の構成例を示す図である。

【図5】図3の2入力縮退回路の構成例を示す図である。

【図6】図3の2入力縮退回路の構成例を示す図である。

【図7】図1の認証システムの動作を説明するタイミングチャートである。

【図8】図1の縮退処理部13の他の構成例を示す図である。

【図9】図8に示す構成例で縮退鍵を生成する場合におけるプロバイダ1の認証システムの構成例を示すブロック図である。

【図10】図8に示す構成例で縮退鍵を生成する場合におけるプロバイダ2の認証システムの構成例を示すブロック図である。

【図11】図8に示す構成例で縮退鍵を生成する場合におけるプロバイダ4の認証システムの構成例を示すブロック図である。

【図12】図9のメモリ11に記憶するデータの生成を説明する図である。

【図13】図10のメモリ11に記憶するデータの生成\*

\*を説明する図である。

【図14】図11のメモリ11に記憶するデータの生成を説明する図である。

【図15】図1の縮退処理部13のさらに他の構成例を示す図である。

【図16】図15に示す方法で縮退鍵を生成する場合のプロバイダ4の認証システムの構成例を示すブロック図である。

【図17】図16の例の動作を説明するタイミングチャートである。

【図18】鍵を変更する場合の動作を説明する図である。

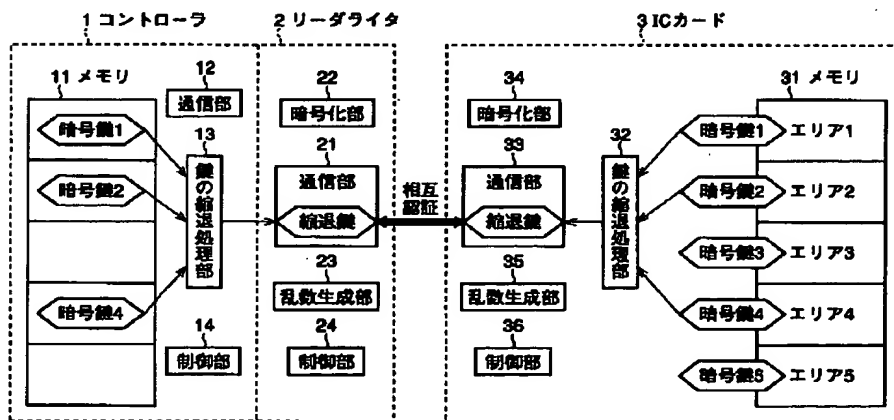
【図19】他の認証処理を説明するブロック図である。

【図20】従来の認証システムの構成を示す図である。

【符号の説明】

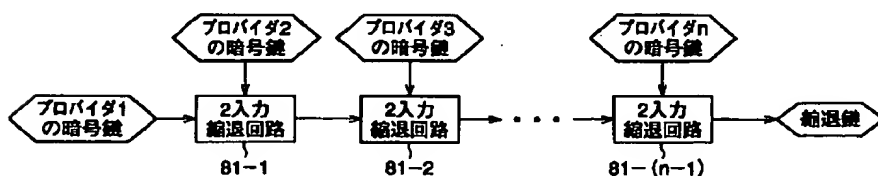
1 コントローラ, 2 リーダライタ, 3 ICカード, 11 メモリ, 12 通信部, 13 縮退処理部, 14 制御部, 21 通信部, 22 暗号化部, 23 乱数生成部, 24 制御部, 31 メモリ, 32 縮退処理部, 33 通信部, 34 暗号化部, 35 乱数生成部, 36 制御部

【図1】

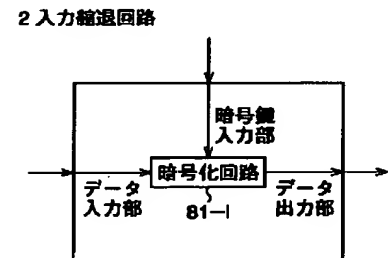


【図3】

縮退鍵生成処理

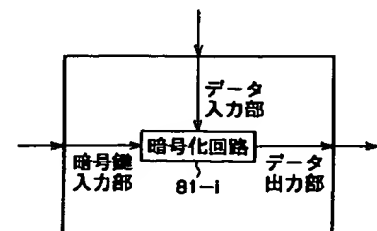


【図4】

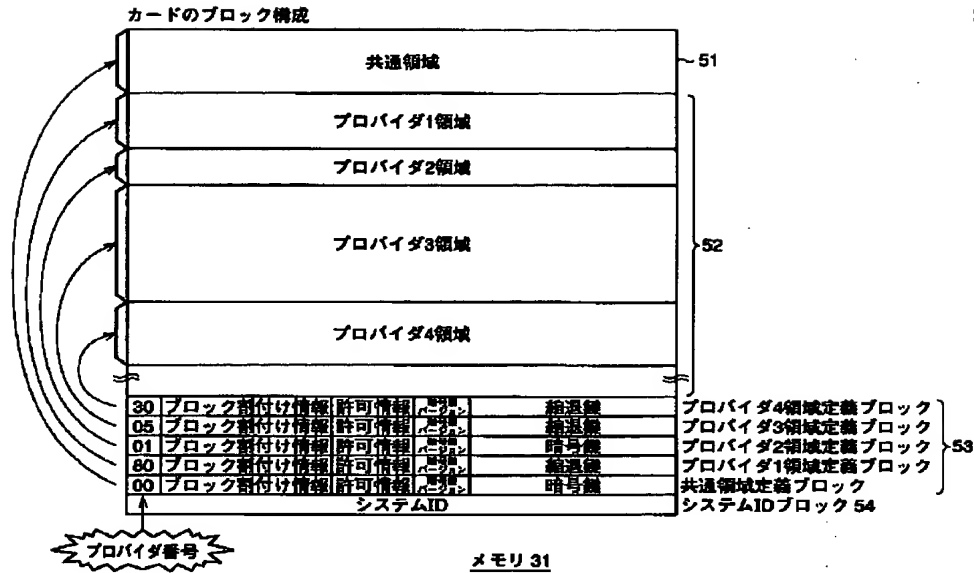


【図5】

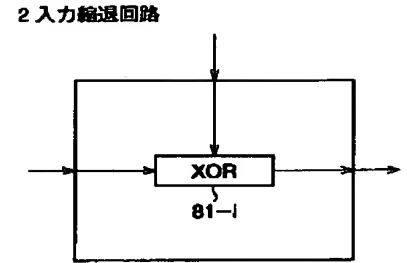
2入力縮退回路



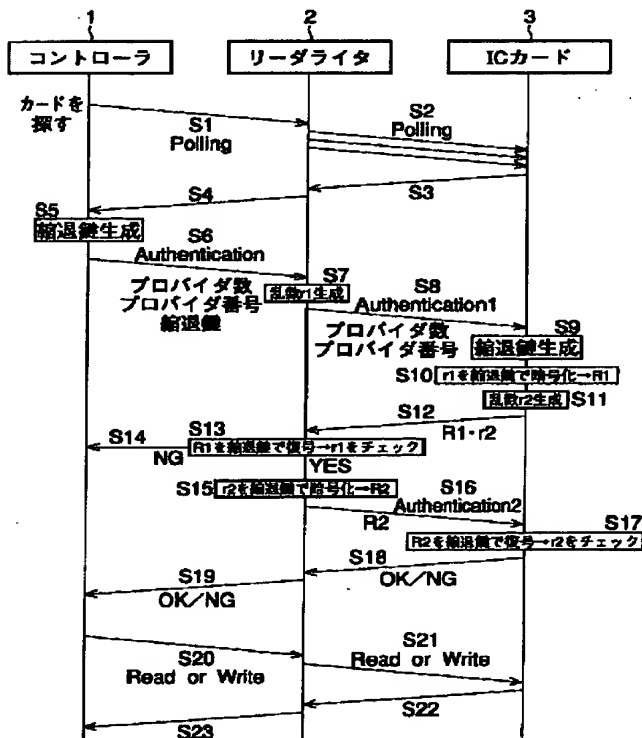
【図 2】



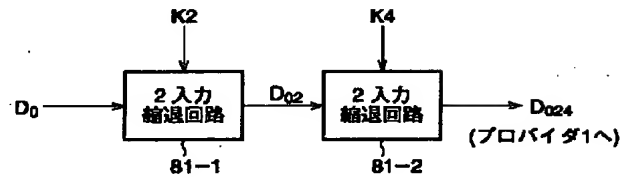
【図 6】



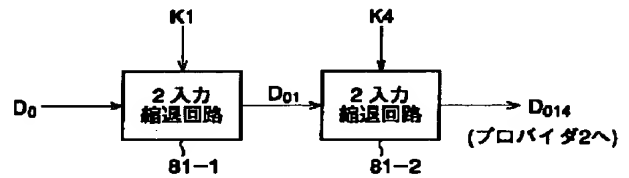
【図 7】



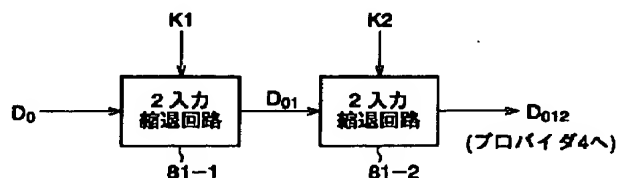
【図 12】



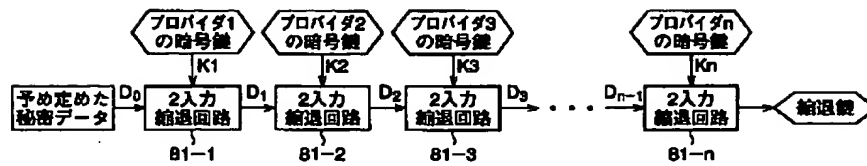
【図 13】



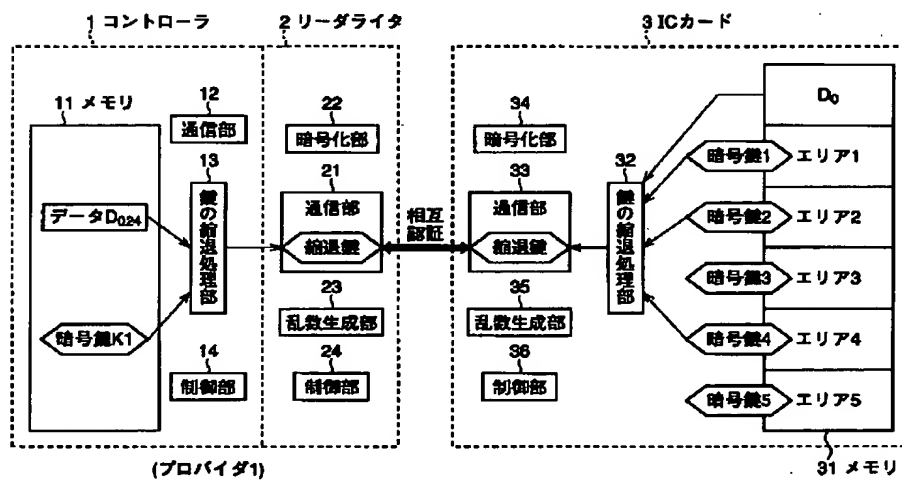
【図 14】



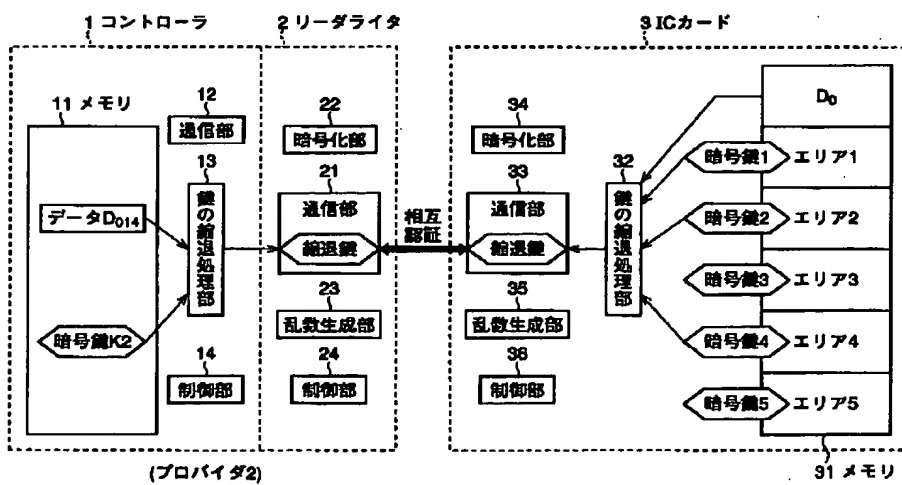
【図8】



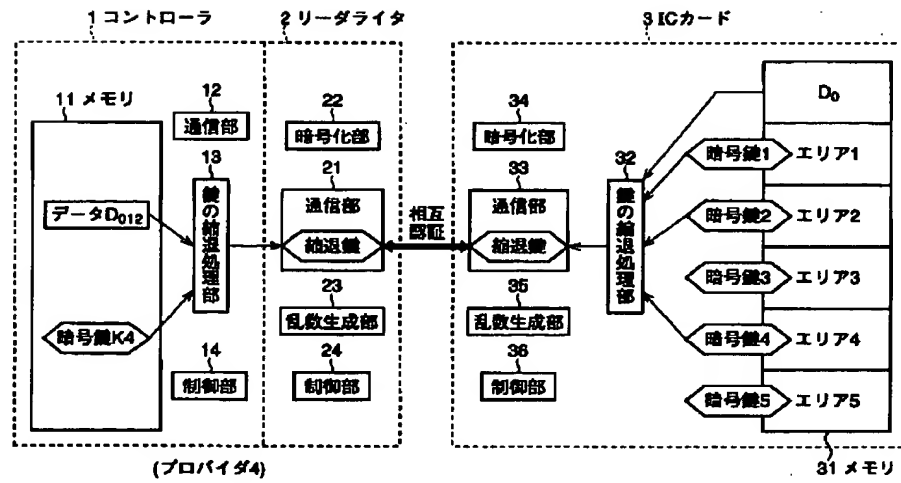
【図9】



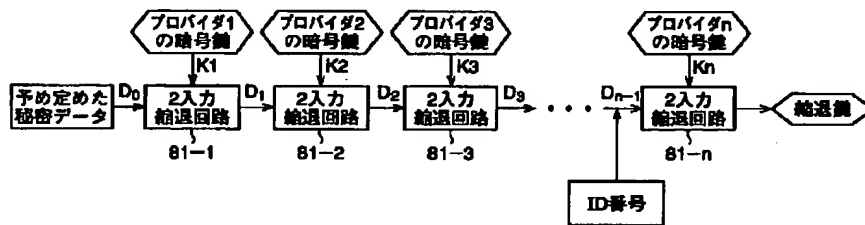
【図10】



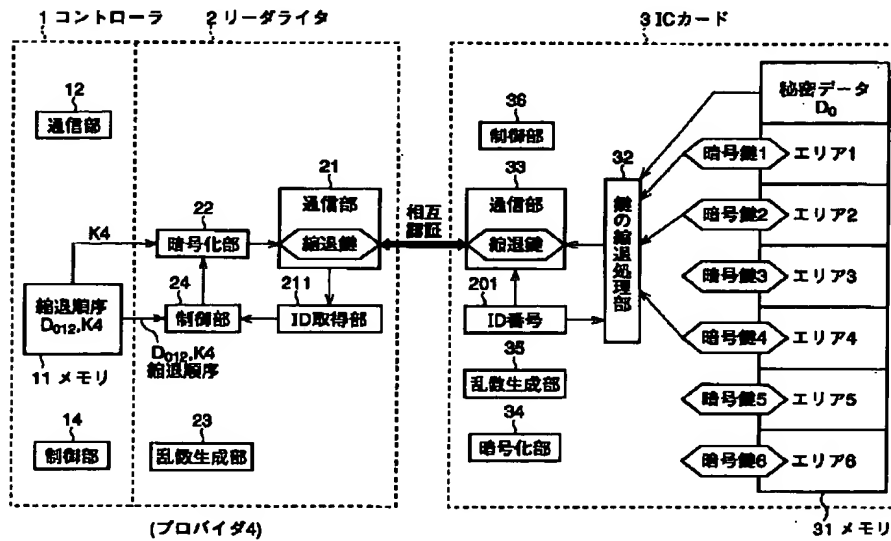
【図11】



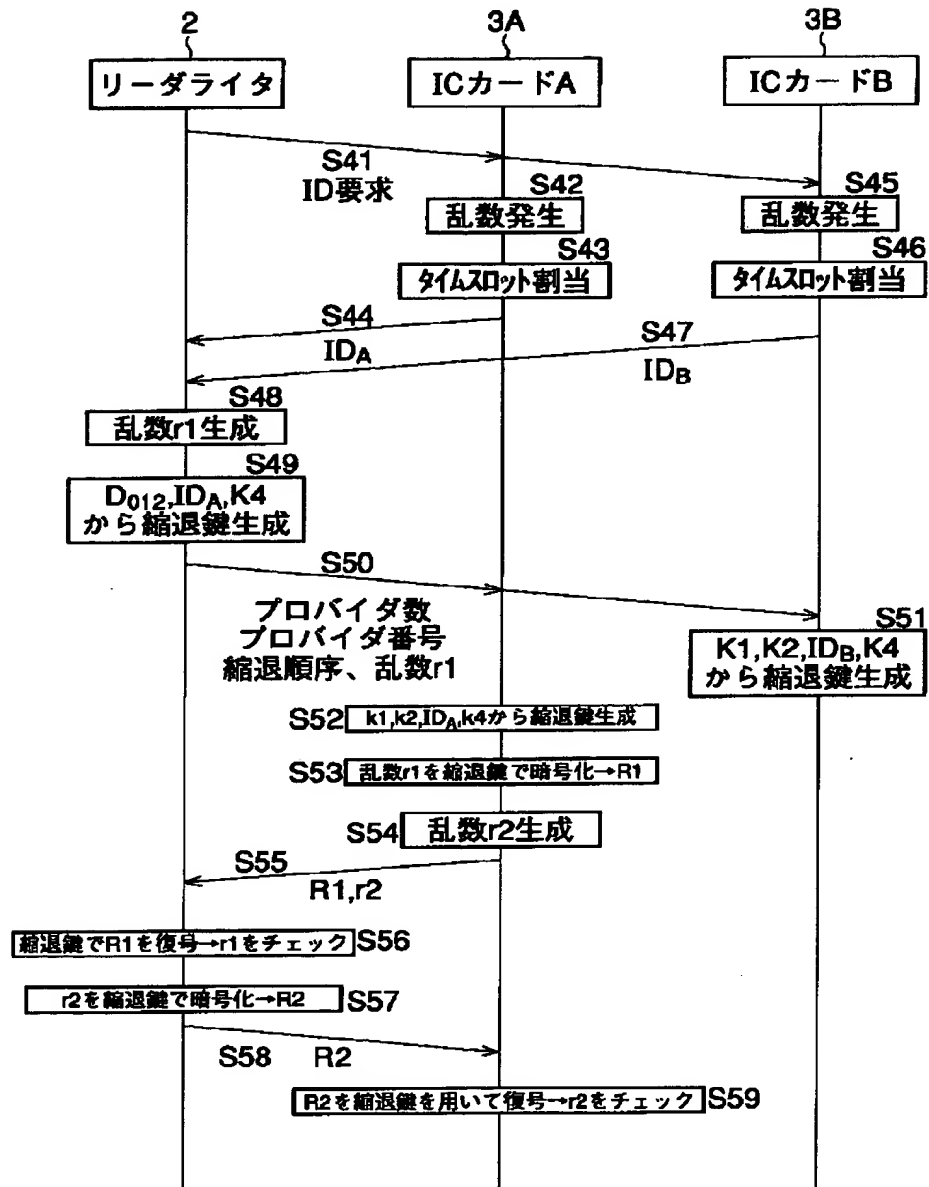
【図15】



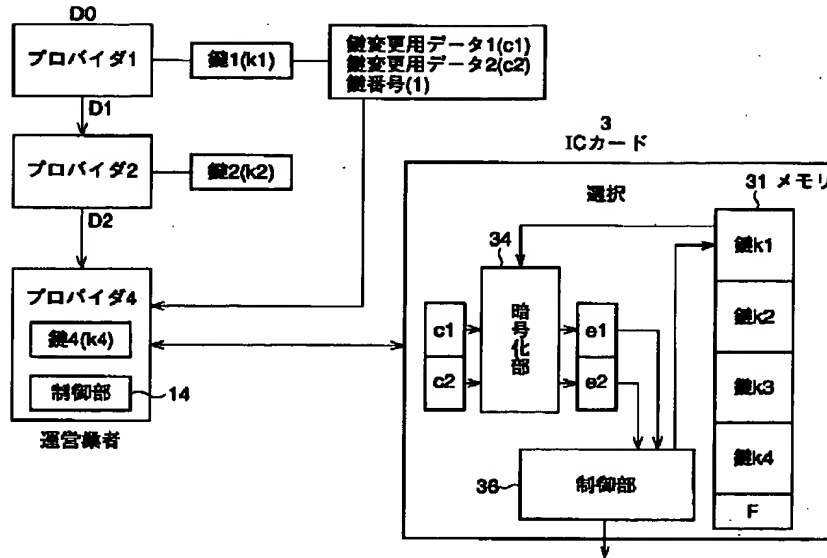
【図16】



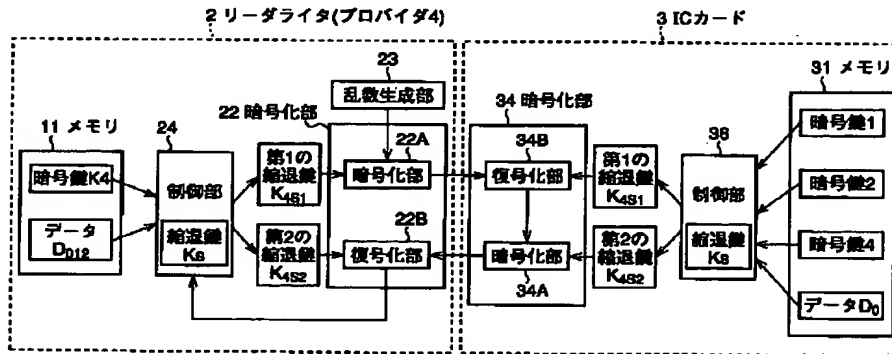
【図17】



【図 18】



【図 19】



【図 20】

